

XOmail

Secure message based information handling

XOmail is a key component in information handling and transfer e.g. as part of C4ISR solutions. The functionality is tailored to messaging tasks in military organisations. XOmail has been continuously improved based on feedback from daily use and from large exercises and operations.

XOmail is updated to the latest versions of NATO STANAG 4406 ("MMHS"). A built-in ACP 127-gateway ensures backwards compatibility.

It integrates with Directory and Public Key Infrastructure components to form complete off-the-shelf solutions.

Optional components for Army and Navy tactical messaging and directory services can implement a true **common service** supporting e.g. headquarters, army task groups and submarines.

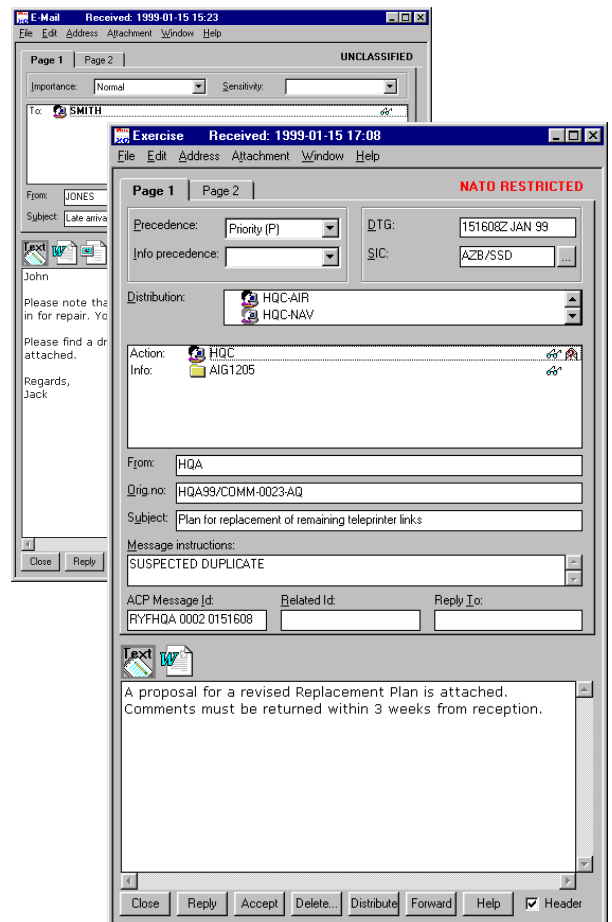
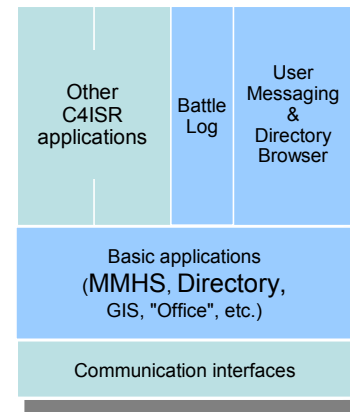
XOmail offers powerful desk-to-desk messaging functions and Battle Log features.

It includes flexible management functions supporting central and/or autonomous (e.g. Wartime) operation.

XOmail is designed as a Multi-Level Secure (MLS) system for certification at CC EAL5.

Key benefits

- Delivered as a turn-key military mail system and as a building block in C4ISR
- Integrated gateways to Army and Naval Tactical messaging services using optimised protocols
- Security gateways for controlled interconnection with external systems
- Integrates with existing systems (ACP 127, NSU TARE, etc.) and the new NATO NMS.
- Integration with Office tools

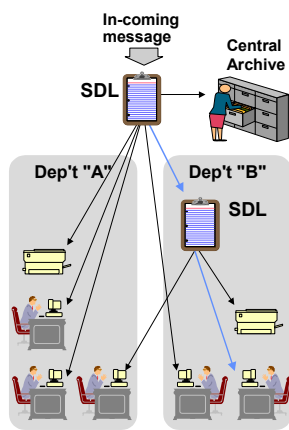


Messaging functions

Messaging functions are tailored to the needs of large organisations. The system differentiates strictly between official messages (to the organisation) and personal messages (to individual users). The user application provides a complete environment for preparation and handling of incoming, outgoing, and stored messages with advanced "workgroup" services, such as *automatic distribution, coordination and release*.

Automatic distribution

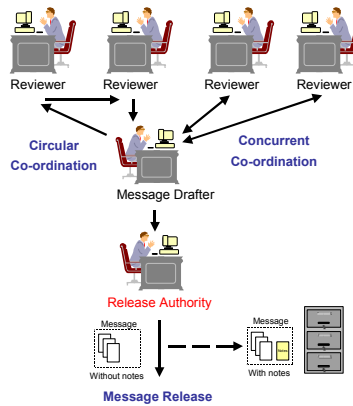
XOmail automatically distributes messages according to the pre-defined Standard Distribution Lists (SDL) of the sending or receiving department.



The distribution is based on criteria such as SIC, Subject, Security Label and ADatP-3 MSGID.

Message coordination and release

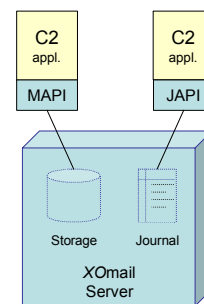
Circular and Concurrent Coordination of messages are available as part of the drafting process.



A Release Authority can be used to either release the message or return it to the drafter with comments.

Interface to applications

XOmail serves other applications through several Application Program Interfaces (APIs). Two such APIs are:



The Messaging API (MAPI) defined by Microsoft is the defacto industry standard.

The Journal API (JAPI) enables applications to file additional information into the Journal.

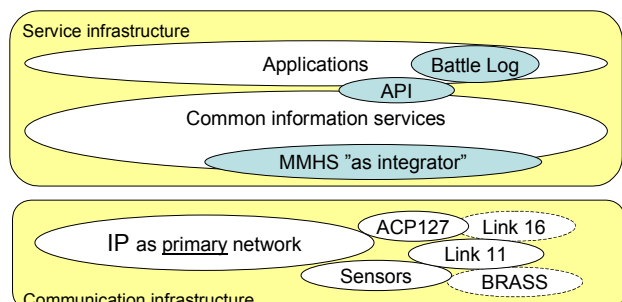
Directory

The integrated ACP 133-based Directory service provides capabilities for the administration of addresses, address lists, certificates, etc. XOmail uses standardized protocols to integrate XOmail nodes and third-party Directory servers in an overall Directory system, e.g. using Shadowing and Chaining.

Military characteristics

Messages are handled according to their precedence both within and between nodes. Higher precedence messages take priority and may suspend lower precedence messages until the resource becomes available. This ensures efficient use of bandwidth even when small high priority messages frequently interrupts other traffic.

XOmail is a middleware component providing a tri-service layer across otherwise incompatible sub-networks in short and medium term NEC solutions.



Security

XOmail has been designed and implemented as a Multi-Level Secure system operating under control of a certified Security Kernel ("Trusted Computing Base"). All messages have a Security Label assigned to them. Individual interfaces are assigned security *label ranges* and *status* (e.g. MLS, System-High with or without advisory Labels).

NATO RESTRICTED

External cryptographic devices can be utilized to ensure that classified messages are transmitted on authorized channels only. Logs, journals, and audit information are automatically generated and stored. Server initiated virus control can be activated.

Messaging Security Services

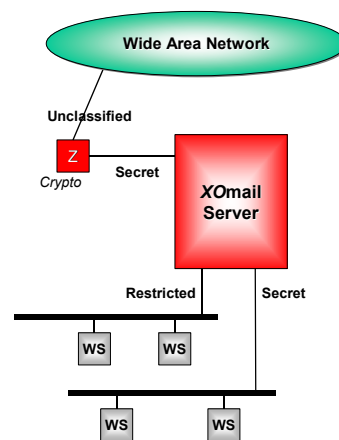
Security services are implemented according to STANAG 4406 using the S/MIME-based PCT-protocol. Digital Signatures are used to ensure that

- the origin can be verified by the recipient
- the message is unaltered
- the originator can have a proof of reception

Certificates are used to carry the signature and optional privileges. A Smart Card is typically used to hold a user's Private Key. Certificates are handled by a replaceable Public Key Infrastructure (PKI).

Secure servers

Utilizing its Multi-Level Security characteristics, XOmail is able to serve as a secure gateway between networks with different security characteristics.



A local server configuration may have one or more segments at different levels, and both classified and non-classified external connections. The secure server will ensure that security is under no circumstances compromised.

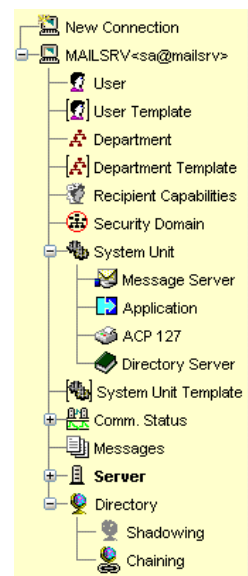
Security Gateways

Manual inspection and re-labelling of messages ("Security Review & Release") from System-High domains are built-in to allow release of messages below the System-High level in a trusted manner. A trusted by-pass option can be used between domains operating with the same policy.

Administration

An administration tool provides powerful functions for setting up and maintaining local components. Groups of users share a common template. New users are added by choosing a predefined template and filling in a few essential parameters. Templates are also available for shared storages and system units.

Remote administration is supported and makes it convenient to administrate a nation-wide service from one or more sites. Inter-node queuing can be supervised and powerful commands allow queued messages to be moved towards another node.



ACP 127 Gateway

- Automatic syntax checking and address conversion
- Automatic generation of channel lists
- Automated ACP 127 channel procedures
- Parallel channels for out-channel "message distribution"
- "Channel Check" generation, looping and supervision
- Format Line 2 TARE AIG/XMT special function

On-line Operation and Maintenance

User-friendly Client for O&M functions:

- User and Department mailboxes
- System Units
 - Servers
 - Applications
 - Gateways
- Automatic functions
 - Distribution
 - Deletion strategies
 - Timeouts
- Performance Management
- Security Management

Central Management

- Performance Management
- Access to Local management functions at any node.

OPTIONS

Central Archive

Long time storage of messages.

Tactical Profile

Allows use of STANAG 4406 Annex E and ACP 142 ("P_MUL") for improved bandwidth utilization.

Optional use of STANAG 5066 or 4538 modems.

MCCIS Gateway

Allows Bi-SC MCCIS messages to be transferred via the MMHS infrastructure.

Broadcast & Ship-Shore Access Unit

- Submarine broadcast
- Vetting
- Automated
 - Screening
 - Traffic list handling
 - CARB
 - Re-run handling
 - Surveillance of messages
 - Broadcast schedules and monitoring



XOmail for Outlook®

Plug-in allowing Outlook users to access XOmail

XOmail TECHNICAL DATA

Baseline specifications

- NATO STANAG 4406
- ACP 133
- ACP 127
- NATO Trusted Computer System Evaluation Criteria
- Common Criteria

Protocols & Interfaces

- S/MIME PCT
- SMTP
- ACP 142 ("P_MUL")
- X.500 DAP/DSP/DISP/DOP
- LDAP
- TCP/IP
- PKCS #7/ #11
- SNMP
- CORBA
- X.25 (option)

Application Program Interfaces

- Journal API
- Messaging API® (MAPI)
- Open Systems ("X/Open") MA and MS APIs (optional STANAG 4406 extensions)

Operating systems

- Windows® 2000/XP/2003
- Solaris® 8, 9, 10 (x86 & Sparc)

2006.02

THALES

THALES NORWAY AS

P.O. Box 6611 Etterstad • NO-0609 Oslo • Norway • Tel: (+47) 22 63 83 00 • Telefax: (+47) 22 63 79 44
<http://XOmail.com/> <http://www.thalesgroup.com/> E-mail: mhs@no.thalesgroup.com